UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,547	03/10/2004	**Blayn W. Beenau**	60655.5900	2546

66170 7590 02/04/2010

Snell & Wilmer L.L.P. (AMEX)
ONE ARIZONA CENTER
400 E. VAN BUREN STREET
PHOENIX, AZ 85004-2202

EXAMINER	
CHAMPAGNE, LUNA	
ART UNIT	**PAPER NUMBER**
3627	

NOTIFICATION DATE	DELIVERY MODE
02/04/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

HSOBELMAN@SWLAW.COM
DMIER@SWLAW.COM
JESLICK@SWLAW.COM

Office Action Summary	Application No.	Applicant(s)	
	10/708,547	BEENAU ET AL.	
	Examiner	Art Unit	
	LUNA CHAMPAGNE	3627	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,19 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,19 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/22/10 has been entered.

Claims 1-17, 19, 20 are presented for examination. Claim 18 is cancelled.

Claim Rejections - 35 USC § 112

2. The rejection of claim 1 under 35 U.S.C. 112, second paragraph, has been reconsidered and the claim is deemed proper as written. Therefore, the rejection is withdrawn.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1–7, 9-12, 14, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seidman et al. (US 6671358 A1), as supported by the provisional (60/286309), in view of Johnson, Jr. (6,185,307 B1), in view of Atalla (4,268,715).

5. Re claim 1, Seidman et al. disclose a system for securing a radio frequency (RF) transaction, the system comprising: a RADIO FREQUENCY IDENTIFICATION (RFID) transaction device operable to send an RF transmission (*See e.g. col. 2, lines 36-42).*

Seidman et al. do not explicitly disclose a system comprising the transaction device including a database for storing a transaction device identifier and a transaction device authentication tag, wherein the transaction device identifier is different from the transaction device authentication tag; a transaction device random number generator for generating a transaction device random number ; a transaction device random number generator for generating a transaction device random number, the transaction device random number generator being located at the transaction device; a transmitter operable to transmit the transaction device identifier, the transaction device authentication tag, and the transaction device random number; wherein the transaction device is validated based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the RFID transaction device; and wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device

authentication tag, the transaction device random number having been received from the RFID transaction device.

However, Johnson JR. discloses a system comprising the transaction device including a database for storing a transaction device identifier and a transaction device authentication tag, wherein the transaction device identifier is different from the transaction device authentication tag (*See e.g. col. 9, lines 1-4);*

a transaction device random number generator for generating a transaction device random number, the transaction device random number generator being located at the transaction device (*see e.g. col. 10, lines 37-39)*;

a transmitter *(transmitter 106)* operable to transmit the transaction device identifier, the transaction device authentication tag, and the transaction device random number (*See e.g. col. 6, lines 33-43)*; wherein the transaction device is validated based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the RFID transaction device (*See e.g. col. 24, lines 44-49 – the code is transmitted to the host 300 to authenticate the tag. Each tag has a different authentication code, which is generated from the tag ID).*

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., and include the steps comprising a transaction device random number generator for generating a transaction device random number , a transmitter operable to transmit the transaction device identifier, the transaction device authentication tag, and the transaction device random number;

wherein the transaction device is validated based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the RFID transaction device; as taught by Johnson JR., in order to further secure transactions and prevent unauthorized interception of valuable information.

Seidman et al., disclose an RFID transaction device. Seidman et al., in view of Johnson JR. do not explicitly disclose the steps wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the RFID transaction device.

However, Atalla discloses the steps and wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device (*see e.g. col. 4, lines 65-67; col. 5, lines 47-54 where, during a transaction, a decryption module at the processing station decrypts an encrypted message sent by a user device using a transmitted random number)*.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., in view of Johnson JR, and include the steps comprising a transaction device random number used to lookup a previously stored decryption key for decrypting at least one of the transaction device

identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device, as taught by Atalla, in order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

6. Re claim 2, Seidman et al. disclose a system further comprising: a RFID reader in communication with said transaction device; a merchant Point of Sale (POS) device in communication with said RFID reader (*See e.g. col. 2, lines 43-47);* and an account authorizing agent in communication with said merchant POS (*See e.g. col. 17, lines 9-12)*.

7. Re claims 3, 4, Seidman et al. disclose a system wherein said RFID reader includes: a reader random number generator for producing a reader random number a system wherein said RFID reader further comprises: a processor in communication with said reader random number generator; and a system wherein a reader database for storing a RFID reader identifier (*See e.g. col. 13, lines 17-25);*

8. Re claim 5, Seidman et al. disclose a system wherein said transaction device random number generator is operable to provide said transaction device random number to said RFID reader, wherein said reader operable to provide said transaction device random number to said POS, wherein said POS configured to provide the

transaction device random number to said account authorizing agent system (*See e.g. col.13, lines 17-25)*.

9. Re claims 6, Seidman et al., disclose system wherein said RFID reader is operable to provide said transaction device identifier to said merchant POS (*See e.g. col. 22, lines 51-59*).

10. Re claims 7 and 12, it would have been a design choice, at the time of the invention, to have at least one of said transaction device identifier and said transaction device random number provided to said RFID reader in track 1/track 2 International Standards Setting Organization format, in order to synchronize the system.

11. Re claim 9, Seidman et al. do not explicitly disclose a system wherein said authorizing agent system is configured to validate said transaction device identifier in accordance with said transaction device random number (*See e.g. col. 18, lines 42-51*).

However, Johnson JR. discloses a system wherein said authorizing agent system is configured to validate said transaction device identifier in accordance with said transaction device random number (*See e.g. col. 11, lines 22-35*).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., and include the steps wherein said authorizing agent system is configured to validate said transaction device identifier in accordance with said transaction device random number, as taught by Johnson JR., in order to authenticate the device.

12. Re claim 10, Seidman et al. disclose a system wherein said RFID reader random number generator is operable to provide said reader random number to said POS, and wherein said POS is configured to provide at least one of said transaction device random number, transaction device identifier, and reader RFID reader random number to said account authorizing agent system (*See e.g. col. 22, lines 48-59, col. 17, lines 9-12)*.

13. Re claims 11 and 14, Seidman et al. disclose a system wherein said RFID reader is operable to provide at least one of said transaction device random number, transaction device identifier, and reader RFID reader random number to said merchant POS; a system wherein said authorizing agent system is configured to validate at least one of said transaction device and said RFID reader, in accordance with said at least one of said transaction device random number, transaction device identifier, and reader RFID reader random number transaction device random number (*See e.g. col. 17, lines 9-42)*.

14. Re claims 19 and 20, Seidman et al., do not explicitly disclose a method wherein the transaction device random number is converted to a validating code and then used to validate the transaction device; a new transaction device random number is generated for each transaction.

However, Johnson JR. discloses a method wherein the transaction device random number is converted to a validating code and then used to validate the transaction device *(see e.g. col. 11, lines 33-35-67);* a new transaction device random number is generated for each transaction *(see e.g. col. 13, lines 65-67)*.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Seidman et al., and include a method wherein the transaction device random number is converted to a validating code and then used to validate the transaction device; a new transaction device random number is generated for each transaction, as taught by Johnson JR., in order to alter the authentication process in such a way that only authorized devices can communicate with each other.

15. Claims 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seidman et al. (US 6671358 A1), as supported by the provisional (60/286309), in view of Johnson, Jr. (6,185,307 B1), in further view of Atalla (4,268,715), in view of further view of Official Notice.

16. Re claims 8 and 13, Seidman et al., in view of Johnson JR., do not explicitly disclose a system wherein at least one of said transaction device identifier and said

transaction device random number is provided to said RFID reader in POS pre-defined format.

However the Examiner takes Official Notice that it is well known in the art that a recognizable format should be provided to a receiving system in a network.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to include a transaction device identifier and wherein said transaction device random number is provided to said RFID reader in POS pre-defined format, in order to synchronize the system.

17. Claims 15 and 16 are rejected under 35 U.S.C. 102(e) as being unpatentable by Johnson, Jr. (6,185,307 B1), in further view of Atalla (4,268,715).

18. Re claim 15, Johnson JR. discloses a method for securing a transaction comprising the steps wherein the transaction device is associated with a transaction (S*ee e.g. col. 10, lines 61-65)*; device identifier and a transaction device authentication tag, the transaction device identifier being different from the transaction device authentication tag (S*ee e.g. col. 10, lines 38-41)*; and transmitting the transaction device identifier, the transaction device authentication tag, and the transaction device random number (S*ee e.g. col. 6, lines 33-43)*: and validating the transaction device based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the transaction device (S*ee e.g. col. 24, lines 44-49)*,

providing a transaction device, the transaction device including a random number generator; generating a transaction device random number (*see e.g. col. 10, lines 37-39)*.

Johnson JR. do not explicitly disclose wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device.

However, Atalla discloses wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device (*See e.g. col. 51, lines 47-54)*.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Johnson JR, and include the steps comprising a transaction device random number used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device, as taught by Atalla, in order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

19. Re claims 16, Johnson et al. disclose a method further comprising the steps of providing a transaction device reader, the reader including a reader random number generator; providing a reader random number generator for generating a reader random number; and validating at least one of the transaction device and the reader in accordance with at least one of the transaction device random number and the reader random number (*See e.g. col. 10, line 65-67, col.11, lines 13, 11-14, 28-35).*

20. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson, Jr. (6,185,307 B1), in view of Seidman et al. (US 6671358 A1), as supported by the provisional (60/286309), in further view of Atalla (4,268,715).

21. Re claim 17, Johnson Jr. discloses a method for securing a transaction comprising the steps of: providing a transaction device (tag unit 100), the transaction device including a random number generator located at the transaction device (see e.g. col. 13, lines 44-46; col. 10, lines 37-39) , wherein the transaction device is associated with a transaction (S*ee e.g. col. 10, lines 61-65)*; device identifier and a transaction device authentication tag, the transaction device identifier being different from the transaction device authentication tag generating a transaction device random number (S*ee e.g. col. 10, lines 38-41)*; and transmitting, from the transaction device, the transaction device identifier, the transaction device authentication tag, and the transaction device random number to the transaction device reader; transmitting, from the transaction device reader, the transaction device identifier, the transaction device authentication tag, the transaction device random number, and the transaction device

authentication tag to an account issuer associated with the transaction device (host 300) (*See e.g. col. 10, lines 41-44)*;

Johnson JR. does not explicitly disclose validating, at the account issuer, the transaction device (*credit/debit card*) based at least in part on both the transaction device identifier (*credit/debit card number*) and the transaction device authentication tag (code 245), both having been received from the transaction device.

However, Seidman et al. disclose validating, at the account issuer, the transaction device (*credit/debit card*) based at least in part on both the transaction device identifier (*credit/debit card number*) and the transaction device authentication tag (code 245), both having been received from the transaction device (*See e.g. col. 18, lines 13-31)*.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to include the steps of validating, at the account issuer, the transaction device based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the transaction device, as taught by Seidman et al., in order to verify the validity of the transaction device.

Johnson JR., in view of Seidman et al. does not explicitly disclose the limitation wherein the transaction device random number is used to decrypt at least one of the transaction device reader authentication tags.

However, Atalla discloses such limitation in col. 5, lines 47-54.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Johnson JR., in view of Seidman et al., and include the steps wherein the transaction device random number is used to decrypt at least one of the transaction device identifier, and the transaction device authentication tag, as taught by Atalla, in order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

Response to Arguments

22. Applicant's arguments with respect to the previous claims have been considered, but are moot in view of the new grounds of rejection. However, the Examiner would like to reiterate the relevance of the prior arts with respect to Applicant's invention. The Examiner disagrees with Applicant's remark that "Johnson teaches against providing the random number generator on the transaction device itself, as its system relies on three independent subsystems.... to obtain a secure transaction"". In column 10, lines 37-39, it is clearly stated that "the POS device 200 generates and sends a random number to the tag100 and to the host 300. See also column 3, line 58 "the random number generated at the POS device". Furthermore, see column 11, lines 11-12: "The POS device 200 generates the random number (CRN). Therefore, it is clearly shown that the generation of random numbers by transaction devices is old and well known.

As stated by Applicant, Johnson teaches a method of obtaining a secure transaction. The elements and procedures disclosed in Applicant's invention are also

disclosed in Johnson. Transmitting data (including a generated random number) in order to be authenticated is old and well known, as taught by Johnson.

Seidman disclose system for conducting a financial transaction using an RF transaction device, and means for securing the transaction. Johnson discloses the actual elements and processes employed for authentication, which includes the specific identifications of the devices and a random number generated by a POS device.

Atalla describes the use of a technique for transmitting messages in a secure manner and also accurate identification of users. Both Atalla and Johnson disclose decrypting data in order to compare and authenticate a sender/device (see Atalla, *e.g. col. 4, lines 65-67; col. 5, lines 47-54 – See Johnson, col. 11, lines 33-35).* The combination of Seidman, Johnson and Atalla, does anticipate Applicants' claimed limitations.

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luna Champagne whose telephone number is (571) 272-7177. The examiner can normally be reached on Monday - Friday 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Florian Zeender can be reached on (571) 272-6790. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luna Champagne/
Examiner, Art Unit 3627

January 27, 2010

/F. Ryan Zeender/

Supervisory Patent Examiner, Art Unit 3627